

	Oldfield Park Junior School		
	Online Safety Policy		
	Date	Author(s)	Notes
Drafted	19.11.2014	AD	To be presented to governors 9.3.2015
Reviewed	December 2015	DG	Reviewed by new Headteacher and although in draft, this policy is in effect
Adopted	February 2016	DG	Policy adopted by FGB
Reviewed	January 2017	SS	Reviewed by new Computing Lead
Reviewed	September 2017	SS	Reviewed by Computing Lead for new academic year
Reviewed	September 2018	SS	Reviewed by Computing Lead for new academic year
Reviewed	September 2019	HM & SS	Reviewed by Computing Lead for new academic year
Governor: Katie Payne (Safeguarding)			
This policy to be reviewed as part of the Safeguarding procedures on an annual basis			

Development / Monitoring / Review of this Policy

This online safety policy has been developed using SWGfL materials by Mrs Davis (previous Computing Subject Leader) and reviewed by Mr Goucher (Headteacher, Co-DTCP) and Miss Miller (current Computing Lead). It is reviewed by:

- Headteacher
- Online Safety Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers

Consultation with the whole school community takes place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This online safety policy was approved by the Governors Sub Committee on:	<i>February 2016</i>
The implementation of this online safety policy will be monitored by the:	<i>Senior Leadership Team</i>
Monitoring will take place at regular intervals:	<i>Annually</i>
The <i>Governors Sub Committee</i> will receive a report on the implementation of the online safety policy generated by the SLT (which will include anonymous details of online safety incidents) at regular intervals:	<i>Annually</i>
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	<i>September 2019</i>
Should serious online safety incidents take place, the following external persons / agencies should be informed:	<i>Local Authority Designated Officer (LADO) Mel Argles, Deputy Safeguarding</i>

The school will monitor the impact of the policy using logs of reported incidents and internet activity logs. It may, on occasion, be appropriate to complete online safety surveys / questionnaires of pupils, parents / carers and staff.

Scope of the Policy

This policy applies to all members of the Oldfield Park Junior School community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of school Computing systems, both in and out of Oldfield Park Junior School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Oldfield Park Junior School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online safety incidents covered by this policy, which may take place outside of Oldfield Park Junior School, but is linked to membership of Oldfield Park Junior School. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Oldfield Park Junior School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Oldfield Park Junior School.

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the SIPP Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor (Katie Payne) and this role is combined with that of the Child Protection/Safeguarding Governor. The role of the Online Safety Governor will include:

- regular meetings with the Safeguarding Officer/Online Safety Coordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors meeting

Headteacher and Senior Leadership Team:

- The Headteacher (Mr Goucher) has a duty of care for ensuring the safety (including online safety) of members of the school community, though some of the day to day responsibility for online safety may be shared with the Online Safety Co-ordinator (Miss Miller).
- The Headteacher and another member of the Senior Leadership Team (Miss Butler) should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority/Palladian Academy Trust disciplinary procedures).
- The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Designated Safeguarding Leads (Mr Goucher, Miss Butler and Mrs Van Roy)

- If an Online Safety disclosure has taken place, it will be the responsibility of the Designated Safeguarding Leads to deal with the incident.
- They are trained in Online Safety issues and are aware of the potential for serious child protection / safeguarding issues to arise from:
 - sharing of personal data
 - access to illegal / inappropriate materials
 - inappropriate on-line contact with adults / strangers
 - potential or actual incidents of grooming
 - peer on peer abuse including cyberbullying.
- For further guidelines, refer to Annex C in Keeping Children Safe In Education September 2018.

Online Safety Coordinator (Miss Miller and the Designated Safeguarding Leads):

- has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority / SWGfL
- liaises with school technical staff
- receives reports of online safety incidents
- reports regularly to Senior Leadership Team

Network Manager / Technical Staff (Miss Miller and Apollo Technology)

The Technical Staff / Co-ordinator for Computing is responsible for ensuring:

- that Oldfield Park Junior School's technical infrastructure is secure and is not open to misuse or malicious attack
- that Oldfield Park Junior School meets required online safety technical requirements and any Local Authority/Palladian Academy Trust Guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher/Online Safety Coordinator for investigation
- that monitoring software / systems are implemented and updated as necessary.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Oldfield Park Junior School online safety policy and practices. They should also know and understand safeguarding policies including the Peer on Peer Abuse policy (for further guidelines, refer to Part 5 in Keeping Children Safe In Education September 2018).
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Designated Safeguarding Leads or Online Safety Coordinator for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety and Acceptable Use policies

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils:

- are responsible for using the Oldfield Park Junior School digital technology systems in accordance with the Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on peer on peer abuse.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Oldfield Park Junior School's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Oldfield Park Junior School will take every opportunity to help parents understand these issues through newsletters, letters, website and information about online safety literature. Parents and carers will be encouraged to support Oldfield Park Junior School in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in Oldfield Park Junior School.

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited
- Key online safety messages are reinforced as part of a programme of assemblies and pastoral activities
- Pupils are taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils are helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies, the internet and mobile devices

- In lessons where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit
- Pupils searches of the internet are restricted by the filtering that is in place throughout the school.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website
- High profile events e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education – The Wider Community

Oldfield Park Junior School will provide opportunities for members of the community to gain from the school's online safety knowledge and experience. This is offered through the Oldfield Park Junior School website and provides online safety information for the wider community.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator will receive regular updates through attendance at external training events (e.g. from SWGfL) and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Safety Coordinator (Miss Miller) or other nominated person will provide advice/guidance/training to individuals as required.

Training – Governors

Governors take part in online safety awareness sessions, with particular importance for those who are members of any subcommittee involved in online safety as part of safeguarding. This is offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents

Technical – Infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- Oldfield Park Junior School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by Apollo Technology who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The school business manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided differentiated user-level filtering allowing different filtering levels for different groups of users – staff / pupils.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Requests for temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems are to be discussed with the headteacher.
- An agreement is in place regarding the extent of personal use that and their family members are allowed on school devices that may be used out of school.
- An agreement is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Teaching staff have been provided with encrypted USB memory sticks for transferring of personal data.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies.
- The school allows:

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>	<i>Yes – with parents’ permission, kept in the office.</i>	<i>Yes – kept in drawer/ locker. Usage in line with Staff Code of Conduct Policy.</i>	<i>Yes – kept in lockers</i>
Full network access	<i>Yes</i>	<i>Yes</i>	<i>Yes</i>			

Internet only						
No network access				Yes	Yes	Yes

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for peer on peer abuse (including cyberbullying) to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner’s Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils’ full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website as part of the general permissions that parents agree to at the start of each academic year. A list of children whose photographs SHOULD NOT be displayed on the website is held in the school office, staff should make themselves aware of these children before publishing photos.
- Written permission from parents or carers will be obtained before pupil’s work can be published on the school website as part of the general permissions that parents agree to at the start of each academic year.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

Oldfield Park Junior School ensures that:

- It has a Data Protection Policy.
- It has paid the appropriate fee to the Information Commissioner’s Office (ICO).
- It has appointed a Data Protection Office (DPO).
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.

- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Request to see all or a part of their personal data held by the data controller.
- There are clear and understood data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be encrypted/ password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓				✓			
Use of mobile phones in lessons		✓						✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones / cameras			✓					✓
Use of other mobile devices e.g. tablets, gaming devices		✓						✓
Use of personal email addresses in school, or on school network		✓						✓
Use of school email for personal emails	✓						✓	
Use of messaging apps		✓					✓	
Use of social media		✓						✓
Use of blogs		✓					✓	

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content.
- Whole class email addresses may be used at KS2.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
 - Systems for reporting and dealing with abuse and misuse
 - Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to proactively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined process.

The school's use of social media for professional purposes will be checked regularly by the Senior Leadership Team to ensure compliance with the school policies.

Unsuitable/Inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyberbullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

Oldfield Park Junior School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions

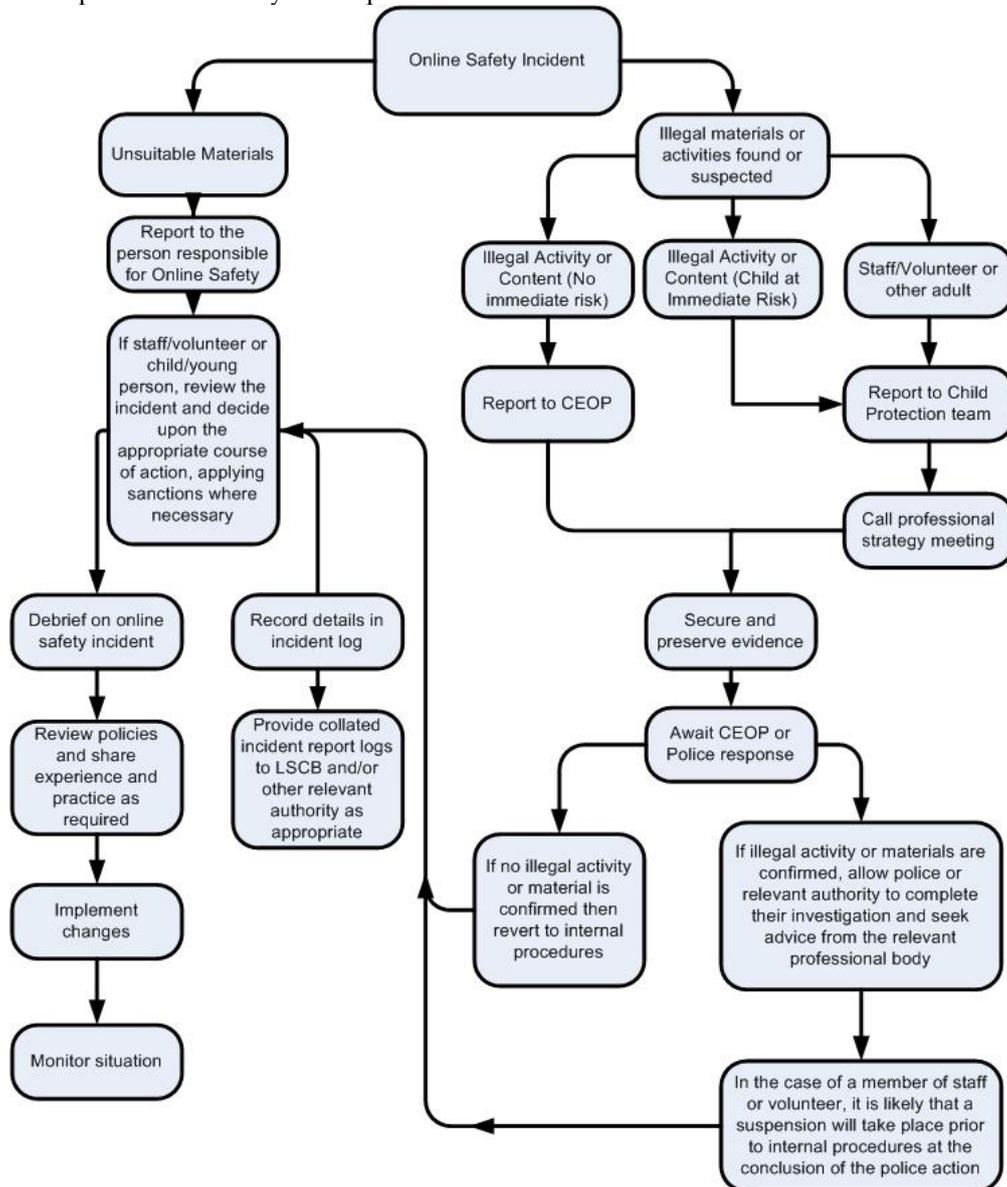
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	promotion of extremism or terrorism				X	
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X		
Using school systems to run a private business				X		
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X		
Infringing copyright				X		
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X		
Creating or propagating computer viruses or other harmful files				X		
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X		
On-line gaming (educational)		X				
On-line gaming (non-educational)		X				
On-line gambling				X		
On-line shopping / commerce		X				
File sharing		X				
Use of social media	X					
Use of messaging apps	X					
Use of video broadcasting e.g. YouTube		X				

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure will be followed:

- More than one senior member of staff will be involved in the process. This is vital to protect individuals if accusations are subsequently reported.
- A designated computer will be used for the procedure that will not be used by young people and if necessary can be taken off site by the police should the need arise. The same computer will be used for the duration of the procedure.
- The relevant staff will have appropriate internet access to conduct the procedure and also the sites and content visited are closely monitored and recorded (to provide further protection).
- The URL of any site containing the alleged misuse will be recorded and the nature of the content causing concern described. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated, the group will judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Palladian Academy Trust or national / local organisation (as relevant).
 - Police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring will be halted and referred to the Police immediately. Other instances to report to the police include:**
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - other criminal conduct, activity or materials

The computer in question will be isolated as any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for Oldfield Park Junior School and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form will be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that Oldfield Park Junior School will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. The following templates illustrate the range of incidents and related actions/sanctions. A completed copy is kept on file at Oldfield Park Junior School.

Pupils

Actions/Sanctions

All the following incidents/actions highlighted below must be referred to the online safety manager and/or Headteacher and may result in any of the actions noted opposite.	Refer to class teacher / tutor	Refer to Deputy Head	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).									
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other mobile device									
Unauthorised use of social media / messaging apps / personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords									
Attempting to access or accessing the school network, using another pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Staff

Actions / Sanctions

Incidents: All the following incidents/actions highlighted below must be referred to the online safety manager and/or Headteacher and may result in any of the actions noted opposite:	Refer to online safety manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).								
Inappropriate personal use of the internet / social media / personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data e.g. holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature								
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy								
Using proxy sites or other means to subvert the school's filtering system inappropriately								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								

Appendix

Copies of the policies and agreements are contained in the appendix and copies of these can be obtained from the school office.

Acknowledgements

Oldfield Park Junior School would like to acknowledge SWGfL and a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School Online Safety Policy Template and of the 360 degree safe e-safety Self Review Tool:

- Members of the SWGfL Online Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

Copyright of these Template Policies is held by SWGfL. Schools / Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy writing, review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL (onlinesafety@swgfl.org.uk) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in April 2018. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© South West Grid for Learning Trust Ltd 2018